# Math 594. Generalized splitting fields and embeddings into a normal extension

Let $E/k$ be an algebraic extension, and $L/k$ a normal extension. Let us assume there exists *at least one* $k$-embedding $E \hookrightarrow L$.

**Theorem 0.1.** *Fix a subextension $E_0/k$ inside of $E/k$. Under the above assumptions, any $k$-embedding $i : E_0 \hookrightarrow L$ lifts to an $E_0$-embedding $j : E \hookrightarrow L$ (viewing $L$ as an extension of $E_0$ via $i$). That is, if $L/k$ is normal and the question of the existence of a $k$-embedding $E$ into $L$ admits an affirmative answer, then the following diagram can always be filled in to be commutative:*

$$\begin{tikzcd}
E \arrow[r, "?"] & L \\
E_0 \arrow[u] \arrow[ur, "i"] & \\
k \arrow[u] \arrow[uur] &
\end{tikzcd}$$

As a special case, if $E = L$ then this says that for any normal extension $L/k$ and any subfield $L_0 \subseteq L$ containing $k$, any $k$-embedding $L_0 \hookrightarrow L$ lifts to a map $L \hookrightarrow L$ which must in fact be an automorphism (since we have seen in class that a self-map of an algebraic extension is necessarily an automorphism). For example, by composing a $k$-automorphism of $L_0$ with the canonical inclusion of $L_0$ into $L$, we see that every $k$-automorphism of $L_0$ lifts to a $k$-automorphism of $L$ (but be careful: not every $k$-automorphism of $L$ will induce an automorphism of $L_0$, unless $L_0$ happens to also be normal over $k$). The normality assumption in the theorem is crucial: if we let $k = \mathbf{Q}$ and $L = \mathbf{Q}(2^{1/4}) = \mathbf{Q}[X]/(X^4 - 2)$ with $x \in L$ the residue class of $X$ modulo $X^4 - 2$, there is no $k$-automorphism of $L$ which lifts the non-trivial automorphism of the subfield $E = \mathbf{Q}(x^2) \simeq \mathbf{Q}(\sqrt{2})$ (proof?).

Now we turn to the proof of the theorem. We begin with a definition which generalizes our earlier notion of splitting field.

**Definition 0.2.** Let $\Sigma$ be a set of non-constant polynomials in $k[T]$. We define a *splitting field of* $\Sigma$ *over* $k$ to be an algebraic extension $k_\Sigma$ of $k$ over which all $f \in \Sigma$ split into a product of linears, and which is generated over $k$ by the roots of all such $f$.

If $\Sigma = \{f_1, \dots, f_n\}$ is finite, it is clear that a splitting field of $\Sigma$ is the same concept as that of a splitting field of the polynomial $\prod f_j$ in our earlier sense. Hence, we see existence and uniqueness up to $k$-isomorphism for finite $\Sigma$. In fact, this works in general:

**Lemma 0.3.** *Let $\Sigma$ be an arbitrary set of non-constant polynomials in $k[T]$. Then a splitting field of $\Sigma$ over $k$ exists and is unique up to $k$-isomorphism. Moreover, an algebraic extension of $k$ is normal if and only if it is the splitting field of some such $\Sigma$.*

*Proof.* It is clear that a splitting field of $\Sigma$ is a compositum over $k$ of splitting fields of each $f \in \Sigma$, so normality of the latter implies normality of the former (recall that an extension of $k$ which is a compositum of finite normal subextensions is itself a normal extension, ultimately because of the real theorem that the splitting field of a polynomial *is* normal). Thus, splitting fields in our generalized sense are necessarily normal over $k$. Conversely, if $L/k$ is a normal extension, then for each $a \in L$ we see (by normality) that $L$ contains a splitting field $L_a/k$ for the minimal polynomial $f_a$ of $a$ over $k$. Thus, $L$ is a splitting field for the set of $f_a$'s. This settles the second part of the lemma.

To handle the existence and uniqueness (up to isomorphism), note (for those who prefer finitistic proofs) that for finite $\Sigma$ we already know both aspects from our earlier work with splitting fields (and the remarks preceding the lemma). To handle the general case, let $\overline{k}$ be an algebraic closure of $k$. Define $k_\Sigma$ to be the subfield of $\overline{k}$ generated over $k$ by all roots of all $f \in \Sigma$. This is clearly a splitting field of $\Sigma$, settling existence. For uniqueness, let $k'$ be a splitting field of $\Sigma$ over $k$. We shall prove that $k'$ is $k$-isomorphic to the explicitly constructed subfield $k_\Sigma$ inside of $\overline{k}$. By algebraicity of $k'$ over $k$, there exists a $k$-embedding $i$ of $k'$ into $\overline{k}$.

Since $k'$ is generated over $k$ by roots of the elements $f \in \Sigma$, $i(k') \subseteq \overline{k}$ is also generated over $k$ by such roots, so $i(k') \subseteq k_\Sigma$. This yields an injection $k' \hookrightarrow k_\Sigma$ which we must prove is surjective.

Let $a \in k_\Sigma$ be the root of some $f \in \Sigma$. Such $a$'s generate $k_\Sigma$ over $k$, so surjectivity of the $k$-map $i$ will follow if each such $a$ lies in $i(k')$. But $k'$ is a splitting field of $\Sigma$ over $k$, so $f$ splits into a product of linears over $k'$. Applying $i$ carries this into a linear factorization of $i(f) = f$ over $k_\Sigma$. One of these latter linear factors must have $a$ as a root. Thus, some linear factor $\ell \in k'[T]$ of $f$ has the property that $i(\ell)$ has $a$ as a root. If $a' \in k'$ is the unique root of the linear $\ell$ in $k'$, then $i(a') \in i(k')$ is the unique root of $i(\ell)$ in $k_\Sigma$. Thus, $i(a') = a$.

∎

Now we prove the theorem.

*Proof.* By the lemma, we can fix a set $\Sigma$ of non-constant polynomials over $k$ for which the normal $L/k$ is a splitting field of $\Sigma$. That is, $L$ is generated over $k$ (and hence over any subfield containing $k$) by roots of the elements of $\Sigma$. Fix a $k$-embedding $j$ of $E$ into $L$. This induces a $k$-embedding $j_0$ of $E_0$ into $L$. Fix an arbitrary $k$-embedding $i$ of $E_0$ into $L$. Viewing $\Sigma$ as a set of polynomials in $E_0[T]$ and using $i$ to embed $E_0$ into $L$ over $k$, $L$ acquires the structure of a splitting field for $\Sigma$ over $E_0$ since $L$ is even generated over $k$ by roots of elements of $\Sigma$ and $i$ is a $k$-embedding. Since both $i$ and $j_0$ make $L$ into a splitting field of $\Sigma$ over $E_0$, by the uniqueness aspect of the lemma we conclude that there exists an automorphism $\sigma$ of $L$ carrying $j_0$ into $i$. Thus, $\sigma \circ j : E \to L$ lifts $i$.

∎